UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,017	02/05/2004	Alan Boulanger	RSW920030105US1	7930

45832 7590 04/11/2008

DILLON & YUDELL LLP
8911 N. CAPITAL OF TEXAS HWY.,
SUITE 2110
AUSTIN, TX 78759

EXAMINER	
DOAN, TRANG T	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
04/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/774,017	BOULANGER ET AL.	
	Examiner	Art Unit	
	TRANG DOAN	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/2004 and 09/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 are pending for consideration.

Information Disclosure Statement

2. The information disclosure statements submitted on 02/05/2004 and 09/09/2005 are being considered by the examiner.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 11-20 and 21-30 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 11-20 are directed to a system comprising the steps of means for detecting, means for applying and means for determining the anomalous traffic. According to the specification, paragraphs 0022 and 0030, the system can be in hardware and/or software. Therefore, claims 11-20 are a system software per se, failing to fall within a statutory category of invention (see MPEP 2106.01).

Claims 21-30 are directed to a computer readable storage medium having computer readable code embodied therein. According to the specification, paragraph 0023, "computer-readable medium .... not limited to, **an electronic, magnetic, optical, electromagnetic, infrared** (e.g., carrier waves, infrared signals, digital signals, etc.) ... computer-readable medium could even be **paper**". In light of the specification, these

claims do not fall within one of the four statutory classes of an invention (method/process, article of manufacture, a composition of matter, or machine). Carrier wave is a signal, not a series of steps. Carrier wave is a form of energy and not a composition of matter. Carrier wave does not have any physical structure, does not itself perform any useful, concrete and tangible result and thus does not fit within the definition of a machine or an article of manufacture.

The dependent claims are depended on the rejected base claim, and are rejected for the same rationales.

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent

and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claims 1-6, 10-16, 20-26 and 30 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-6, 10-15 and 19-24 of copending Application No. 10774140. Although the conflicting claims are not identical, they are not patentably distinct from each other because both applications are claiming common subject matter, which is detecting an anomaly in the communication traffic, applying a first blocking measure A to the anomalous traffic and determining a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous traffic, as follows (similarities are shown using **bold**).

Instant Application 10708004	Copending Application 10774140
Claim 1. A method of operating a communication network, comprising: **detecting an anomaly in communication traffic** at a plurality of nodes in the communication network; independently **applying at**	Claim 1. A method of processing communication traffic, comprising: **detecting an anomaly in the communication traffic**; **applying a first blocking measure A to the anomalous traffic** that stops the

respective ones of the plurality of nodes a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and independently **determining at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous traffic**.	anomalous traffic; and **determining a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous traffic**.
Claim 2. The method of claim 1, wherein independently determining the second blocking measure B comprises: **applying a logical combination of A and a second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and enforcing the logical combination (A & !B) if the logical combination (A & !B) stops the anomalous traffic**.	Claim 2. The method of claim 1, wherein determining the second blocking measure B comprises: **applying a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and enforcing the logical combination (A & !B) if the logical combination (A & !B) stops the anomalous traffic**.
Claim 3. The method of claim 2, further comprising: independently **determining a third blocking measure C at the respective ones of the plurality of nodes such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & !B) stops the anomalous traffic**.	Claim 3. The method of claim 2, further comprising: **determining a third blocking measure C such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & !B) stops the anomalous traffic**.
Claim 4. The method of claim 2, wherein	Claim 4. The method of claim 2, wherein

independently determining the second blocking measure B further comprises: **applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and enforcing the logical combination (A & B) if the logical combination (A & B) stops the anomalous traffic.**	determining the second blocking measure B further comprises: **applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and enforcing the logical combination (A & B) if the logical combination (A & B) stops the anomalous traffic.**
Claim 5. The method of claim 4, further comprising: independently **determining a third blocking measure C at the respective ones of the plurality of nodes such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) stops the anomalous traffic.**	Claim 5. The method of claim 4, further comprising: **determining a third blocking measure C such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) stops the anomalous traffic.**
Claim 6. The method of claim 4, further comprising: **determining a third blocking measure C at the respective ones of the plurality of nodes such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) does not stop the anomalous traffic.**	Claim 6. The method of claim 4, further comprising: **determining a second blocking measure C such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) does not stop the anomalous traffic.**

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Objections

8. Claims 1, 10-11, 20-21 and 30 are objected to because of the following informalities:

Regarding claims 1, 10-11, 20-21 and 30, the limitation "such that application a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous traffic" should be changed to " such that application a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic ".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chi (US 6006329) (hereinafter Chi) in view of Milliken et al. (US 20040064737) (hereinafter Milliken).

Regarding claim 1, Chi discloses a method of operating a communication network, comprising: detecting an anomaly in communication traffic at a plurality of nodes in the communication network (Chi: See Summary section and column 3 lines 35-46: to detect the viruses, each data stream is scanned only for components of a

virus); independently applying at respective ones of the plurality of nodes a first blocking measure A to the anomalous traffic that stops the anomalous traffic (Chi: See figure 3b, column 4 lines 25-48 and column 6 lines 53-67); and independently determining at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B (Chi: See figure 5).

Chi only discloses the detecting method using Boolean expression. Chi does not explicitly disclose stopping the anomalous traffic after the detection method. Milliken discloses stopping the anomalous traffic (Milliken: paragraphs 0031-0032: remedial actions may include disabling the link carrying the malicious traffic, discarding packets coming from a particular source address or discarding packets addressed to a particular destination). It would have been obvious to one with ordinary skill in the art to stop malicious traffic when the malicious traffic has been detected because both prior art disclose the detecting method and stopping method. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Milliken within the system of Chi because there is a need for new defenses to thwart the attack of polymorphic viruses and worms (Milliken: paragraph 0005).

Regarding claims 2, 12 and 22, Chi as modified discloses wherein independently determining the second blocking measure B comprises: applying a logical combination of A and a second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a

logical combination (A & B); and enforcing the logical combination (A & !B) if the logical combination (A & !B) stops the anomalous traffic (Chi: See figure 5 and column 5 lines 5-30 / Milliken: paragraphs 0031-0032). The same motivation was utilized in claim 1 applied equally well to claims 2, 12 and 22.

Regarding claims 3, 13 and 23, Chi as modified discloses independently determining a third blocking measure C at the respective ones of the plurality of nodes such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & !B) stops the anomalous traffic (Chi: See figure 5 and column 6 lines 53-67 / Milliken: paragraphs 0031-0032). The same motivation was utilized in claim 1 applied equally well to claims 3, 13 and 23.

Regarding claims 4, 14 and 24, Chi as modified discloses wherein independently determining the second blocking measure B further comprises: applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and enforcing the logical combination (A & B) if the logical combination (A & B) stops the anomalous traffic (Chi: See figure 5 and Milliken: paragraphs 0031-0032). The same motivation was utilized in claim 1 applied equally well to claims 4, 14 and 24.

Regarding claims 5, 15 and 25, Chi as modified discloses independently determining a third blocking measure C at the respective ones of the plurality of nodes such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B)

stops the anomalous traffic (Chi: See figure 5 and Milliken: paragraphs 0031-0032). The same motivation was utilized in claim 1 applied equally well to claims 5, 15 and 25.

Regarding claims 6, 16 and 26, Chi as modified discloses determining a third blocking measure C at the respective ones of the plurality of nodes such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) does not stop the anomalous traffic (Chi: See figure 5 and column 4 lines 10-48 / Milliken: paragraphs 0031-0032). The same motivation was utilized in claim 1 applied equally well to claims 6, 16 and 26.

Regarding claims 7, 17 and 27, Chi as modified discloses wherein detecting an anomaly in the communication traffic comprises: comparing the communication traffic to at least one anomaly factor; and detecting the anomaly in the communication traffic at the plurality of nodes in the communication network if the at least one anomaly factor is present in the communication traffic (Chi: See figure 5 and Summary section).

Regarding claims 8, 18 and 28, Chi as modified discloses assigning a severity to the detected anomaly; and wherein independently applying the first blocking measure A to the anomalous traffic comprises independently applying the first blocking measure A to the anomalous traffic at each of the plurality of nodes in the communication network that stops or reduces the flow of the anomalous traffic based on the severity of the detected anomaly (Chi: See figure 5 and Summary section / Milliken: paragraphs 0031-0032). The same motivation was utilized in claim 1 applied equally well to claims 8, 18 and 28.

Regarding claims 9, 19 and 29, Chi as modified discloses intentionally inserting the anomaly in the communication traffic; and associating the first blocking measure A and the second blocking measure B with the anomaly (Chi: See figure 5 and Summary section).

Regarding claim 10, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 11, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 20, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 21, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 30, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2131

/Christopher A. Revak/
Primary Examiner, Art Unit 2131